11

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/823,423	03/29/2001	Michael S. Ripley	42390P10855	9405

8791 7590 05/31/2006

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 05/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.	Applicant(s)	
09/823,423	RIPLEY ET AL.	
Examiner	**Art Unit**	
Tom Gyorfi	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,11-16,18-21 and 23-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9,11-16,18-21 and 23-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-9, 11-16, and 18-26 remain for examination. The correspondence filed 3/6/06 amended claims 1, 11, and 18; and cancelled claims 10, 17, and 22.

Response to Arguments

2. Applicant's arguments with respect to claims 1-26 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 1-9, 11-16, 18-21, and 23-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nagai et al (U.S. Pre-grant Publication 2002/0015494).

Regarding claim 1:

Nagai discloses a system comprising: a number generator housed in a host device to generate a nonce (element 250 of Figure 2B, and paragraph 0167); and an encryption subsystem housed in a storage device (element 914 of Figure 10) containing a key distribution data block (paragraph 0055) using an encryption bus key prior to transmitting the encrypted data via a data bus to the host device in which the encrypted data is to be decrypted (paragraphs 0122-0123).

Although Nagai does not describe how the bus key is generated, it describes a method wherein a title key is derived based on [1] a portion of the key distribution data block, [2] a device key assigned to said encryption subsystem and [3] the nonce received over the data bus from the number generator (paragraphs 0059-0065). It would have been obvious to generate the disclosed bus key in a similar fashion, as doing so allows the invention to be suitable for digital broadcast systems using wireless broadcasts (paragraph 0065).

Regarding claim 11:

Nagai discloses a method comprising:

a storage device reading a key distribution data block from a storage medium (Figure 2A);

the storage device processing at least a portion of said key distribution data block using least one device key to compute a media key (paragraph 0063);

the storage device fetching a nonce received over a data bus from a number generator housed in a host device (paragraph 0167 and element 250 of Figure 2B);

encrypting data read from the storage medium using the generated bus key (paragraph 00175); and

the storage device transmitting the encrypted data over a data bus to the host device in which the encrypted data is to be decrypted (Ibid).

Although Nagai does not describe how the bus key is generated, it describes a method wherein the storage device combining said nonce with said media key using a one-way function to generate a key (paragraph 0063-0065 and 0167-0168). It would have been obvious to generate the disclosed bus key in a similar fashion, as doing so allows the invention to be suitable for digital broadcast systems using wireless broadcasts (paragraph 0065).

Regarding claim 18:

Nagai discloses an apparatus comprising: a storage device to access a storage medium containing data and a key distribution data block (Figure 2A), said storage device including a processing logic, a one-way function and an encryption logic (Figure 10), wherein said processing logic processes a portion of said key distribution data block using a device key assigned to said storage device to compute a media key (parargraphs 0059-0065), said one-way function combines said media key with a nonce received over a data bus from a number generator housed in a host device (Ibid, and paragraphs 0167-0168) prior to transmitting the encrypted data via the data bus to the host device in which the encrypted data is to be decrypted.

Although Nagai does not describe how the bus key is generated, it describes a method wherein the storage device combining said nonce with said media key using a one-way function to generate a key (paragraph 0063-0065 and 0167-0168). It would have been obvious to generate the disclosed bus key in a similar fashion, as doing so allows the invention to be suitable for digital broadcast systems using wireless broadcasts (paragraph 0065).

Regarding claim 19:

Nagai discloses or suggests the limitations of claim 18 above. Nagai further discloses a host device coupled to said storage device via said data bus (Figure 10), said host device including a processing logic, a one-way function and a decryption logic (Ibid, and Figures 2A-2B), wherein said processing logic processes a portion of said key distribution of said key distribution data block using a device key assigned to said host device to compute a media key (paragraphs 0063-0065), said one-way function combines said media key with said nonce generated by said number generator to produce a bus key (paragraphs 0059-0065, and 0167-0168) and said decryption logic decrypts said encrypted data received over the data bus using said bus key (paragraph 0141).

Regarding claim 2:

Nagai discloses or suggests all the limitations of claim 1 above. Nagai further suggests a decryption subsystem coupled to said data bus to decrypt said encrypted data received over the data bus using a decryption bus key derived based on [1] a portion of the key distribution data block, [2] a device key assigned to said encryption subsystem and [3] the nonce received over the data bus from the number generator (element 918 of Figure 10; and paragraphs 0059-0065).

Regarding claim 3:

Nagai discloses or suggests all the limitations of claim 1 above. Nagai further discloses a processing logic to process at least a portion of the key distribution data block read from the storage medium using the device key assigned to said encryption subsystem to compute a media key (element 912 of Figure 10); a one way function to generate the encryption bus key based on the media key and the nonce generated by the number generator (paragraphs 0167-0168); and an encryption logic to encrypt data accessed from said storage medium using said encryption bus key (element 910 of Figure 10).

Regarding claim 4:

Nagai discloses or suggests the limitations of claim 2 above. Nagai further discloses a processing logic to process at least a portion of the key distribution data block read from the storage medium using the device key assigned to said decryption subsystem to compute a media key (element 905 of Figure 10); a one way function to generate the encryption bus key based on the media key and the nonce generated by the number generator (paragraphs 0167-0168); and an decryption logic to decrypt data transmitted over the data bus by using said decryption bus key (element 918 of Figure 10) (see also Figure 14).

Regarding claims 5, 12, and 20:

Nagai discloses or suggests the limitations of claims 5, 11, and 18 above. Nagai further discloses wherein said data transmitted over the data bus is encrypted using the bus key derived based on the nonce generated by the number generator such that if said data is recorded at the time of transmission, said recorded data is not subsequently playable by a decryption subsystem that does not have access to the same nonce used by said encryption subsystem to encrypted said data transmitted over the data bus (paragraphs 0140 and 0145-0146).

Regarding claims 6, 16, and 26:

Nagai discloses or suggests the limitations of claims 2, 11, and 19 above. Nagai further discloses wherein said key distribution data block is embodied in the form of a media key block comprising a block of encrypted data (paragraph 0062).

Regarding claim 7:

Nagai discloses or suggests the limitations of claim 2 above. Nagai further discloses wherein said encryption subsystem is implemented in a storage device capable of accessing data from a storage medium and said decryption subsystem is implemented in a host device capable of retrieving data from said storage device (Figure 10; paragraph 0136).

Regarding claims 8 and 21:

Nagai discloses or suggests the limitations of claims 2 and 19 above. Nagai further discloses wherein said media key computed by the said encryption subsystem will be the same as the media key computed by the decryption subsystem provided that neither the device key assigned to the encryption subsystem nor the device key assigned to the decryption subsystem have been compromised (paragraphs 0063-65).

Regarding claims 9 and 24:

Nagai discloses or suggests the limitations of claim 2 and 19 above. Nagai further discloses wherein said storage medium is selected from a digital versatile disc (DVD), CD-ROM, optical disc, magneto-optical disc, flash-based memory, magnetic card, and optical card (paragraphs 0039-0040 and 0180).

Regarding claim 13:

Nagai discloses or suggests the limitations of claim 11 above. Nagai further discloses decrypting the encrypted data received over the data bus (paragraph 0145).

Regarding claim 14:

Nagai discloses or suggests the limitations of claim 13 above. Nagai further discloses wherein said decrypting the encrypted data received over the data bus comprises:

a host device reading a key distribution data block from a storage medium (Figure 2A-2B);

the host device processing at least a portion of said key distribution data block using least one device key to compute a media key (paragraph 0063);

the host device fetching the nonce generated by the number generator (paragraph 0167 and element 250 of Figure 2B);

the host device combining said media key with the nonce using a one-way function to generate a bus key (paragraphs 0059-0065 and 0167-0168);

the host device decrypting said encrypted data received over the data bus using the bus key generated by the host device (paragraph 0141).

Regarding claim 15:

Nagai discloses or suggests the limitations of claim 14 above. Nagai further discloses the host device requesting a descramble key required for descrambling scrambled content from said storage device (paragraph 0145); the storage device encrypting said descramble key read from said storage medium with said bus key generated by said storage device and sending said encrypted descramble key to the host device (Ibid); the host device descrambling said encrypted descramble key received from said storage device using said bus key generated by said host device (Ibid); the host device descrambling said decrypted data using said descramble key decrypted by said host device (paragraph 0141).

Regarding claim 23:

Nagai discloses or suggests the limitations of claim 19 above. Nagai further discloses wherein said storage device is embodied in the form of a DVD drive and said host device is embodied in the form of either a DVD player or personal computer (paragraph 00136).

Regarding claim 25:

Nagai discloses or suggests the limitations of claim 19 above. Nagai further discloses wherein said storage medium is embodied in the form of a DVD containing scrambled content (paragraphs 0038-0040).

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- U.S. Patents 6,950,941 to Lee; 6,832,319 to Bell; 6,550,011 to Sims III; and 6,542,610 to Traw
- PCT Publication WO 98/45980 to Fielder et al.
- "Handshake Protocol for Data Privacy Keys" IBM Technical Disclosure Bulletin April 1992, Volume 34, Issue 11. (This reference further establishes that one-way functions were well known in their use to establish a shared bus key as confidential functions (see page 2 as indicated).

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TAG
5/26/06

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100